UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

August Term, 2018

Argued: August 27, 2018 Decided: December 18, 2019

Docket No. 15-2684-L; 17-2669-CON

UNITED STATES OF AMERICA,

Appellee,

— v. —

AGRON HASBAJRAMI,

Defendant-Appellant.

Before:

LYNCH, CARNEY, and DRONEY, *Circuit Judges.*

Agron Hasbajrami was arrested at John F. Kennedy International Airport in September 2011 and charged with attempting to provide material support to a terrorist organization. After he pleaded guilty, the government disclosed, for the first time, that certain evidence involved in Hasbajrami's arrest and prosecution had been derived from information obtained by the government without a warrant pursuant to its warrantless surveillance program under Section 702 of the FISA Amendments Act of 2008. Hasbajrami then withdrew his initial plea

and moved to suppress any fruits of the Section 702 surveillance. The district court (Gleeson, then-*J.*) denied the motion to suppress and Hasbajrami again pleaded guilty, this time pursuant to a conditional guilty plea that allowed him to appeal the district court's ruling denying his motion to suppress.

He now appeals, arguing *inter alia* that the warrantless surveillance and the collection of his communications violated the Fourth Amendment. We conclude that the collection of the communications of United States persons incidental to the lawful surveillance of non-United States persons located abroad does not violate the Fourth Amendment and that, to the extent that the government's inadvertent targeting of a United States person led to collection of Hasbajrami's communications, he was not harmed by that collection. [redacted] Because there is insufficient information in either the classified or the public record in this case to permit us to determine whether any such querying was reasonable, and therefore permissible under the Fourth Amendment, we REMAND the case to the district court for further proceedings consistent with this opinion.

MICHAEL K. BACHRACH, Law Office of Michael K. Bachrach, New York, NY, Joshua L. Dratel, Joshua L. Dratel, P.C., New York, NY, and Steve Zissou, Steve Zissou & Associates, Bayside, NY, *for Defendant-Appellant Agron Hasbajrami.*

SETH D. DUCHARME, David C. James, Saritha Komatireddy, Assistant United States Attorneys, Joseph F. Palmer, Attorney, National Security Division, United States Department of Justice *for* Richard P. Donoghue, United States District Attorney for the Eastern District of New York, Brooklyn, NY, *for the United States of America.*

PATRICK TOOMEY and Ashley Gorski, American Civil Liberties Foundation, New York, NY, Mark Rumold and Andrew Crocker, Electronic Frontier Foundation, San Francisco, CA, *Amici Curiae American Civil Liberties Union and Electronic Frontier Foundation.*

GERARD E. LYNCH, *Circuit Judge*:

This case concerns the Fourth Amendment implications of the government's increasing technological capacity for electronic surveillance in foreign intelligence and terrorism investigations, and the balance our constitutional system requires between national security and individual privacy.

On September 6, 2011, Defendant-Appellant Agron Hasbajrami ("Hasbajrami") was arrested as he attempted to board a flight to Turkey at John F. Kennedy International Airport in Queens, New York. His luggage contained a tent, boots, and cold-weather gear. The government, which had collected Hasbajrami's electronic communications, charged him with attempting to provide material support to a terrorist organization, alleging that he intended to travel to the Federally Administered Tribal Area of Pakistan, where he expected to join a terrorist organization, receive training, and ultimately fight "against U.S. forces and others in Afghanistan and Pakistan." App'x at 44. During the course of the prosecution, the government disclosed that it had collected some of its

evidence under the Foreign Intelligence Surveillance Act of 1978 ("FISA"), Pub. L. No. 95-511, 92 Stat. 1783 (1978), codified at 50 U.S.C. § 1801 *et seq.*, and that it intended to introduce FISA-derived evidence at any eventual trial. Faced with the evidence, including his own incriminating communications, Hasbajrami ultimately pleaded guilty to attempting to provide material support to terrorists in violation of 18 U.S.C. § 2339A. He was sentenced to 180 months in prison.

Hasbajrami was already serving his sentence when the government provided him with a supplemental letter disclosing, for the first time, that some of the evidence it had previously disclosed from FISA surveillance was itself the fruit of earlier information obtained without a warrant pursuant to Section 702 of the FISA Amendments Act ("Section 702"), Pub. L. No. 110-261, 122 Stat. 2436 (2008), codified at 50 U.S.C. § 1881a.

It is that Section 702-derived evidence — primarily electronic communications between Hasbajrami and individuals without ties to the United States and located abroad — that is at issue in this appeal. Following the disclosure of Section 702 surveillance, the district court (John Gleeson, then-*J.*) permitted Hasbajrami to withdraw his plea; Hasbajrami subsequently moved to suppress all evidence seized by the government under its Section 702 programs,

as well as any fruits of that surveillance, including the evidence obtained pursuant to FISA warrants and inculpatory statements Hasbajrami made upon arrest. The district court denied the motion to suppress, and Hasbajrami again pleaded guilty, reserving his right to appeal the district court's denial of his suppression motion.

The vast majority of Section 702 surveillance at issue here involves information the government collected about Hasbajrami incidental to its surveillance of other individuals without ties to the United States and located abroad. [redacted][1]

[1] This opinion has been reviewed by appropriate intelligence agencies for the purpose of redacting material that includes or references classified information. After an initial redaction, the panel met *ex parte* with representatives of those agencies in order to discuss potential substitutions or modified phrasing that would minimize the need for redaction, and the possibility that certain information referenced in the opinion could be declassified, thus further

In light of that disclosure, and the evidence in the public and classified record, we reach three principal conclusions:

> *First*, the "incidental collection" of communications (that is, the collection of the communications of individuals in the United States acquired in the course of the surveillance of individuals without ties to the United States and located abroad) is permissible under the Fourth Amendment. We therefore conclude, in agreement with the district court, that, at least insofar as the record available to the district court is concerned, the vast majority of the evidence detailed in the record was lawfully collected.
>
> *Second*, the "inadvertent collection" of communications of those located within the United States (that is, the acquisition of communications accidentally collected because an intelligence agency mistakenly believes that an individual is a non-United States person located abroad and therefore targets that individual's e-mail address under its Section 702 authority) raises novel constitutional questions. We do not reach those

---

reducing the need for redaction. That meeting was transcribed for the record, and the transcript (which is itself classified) will be preserved as part of the record of this appeal in the custody of a Classified Information Security Officer with the Department of Justice's Litigation Security Group. The meeting was extremely productive, and has resulted in a modest number of changes of wording that do not affect the substance of the opinion, and a significant reduction in the amount of redacted material. It is of course regrettable that any part of an opinion disposing of a criminal appeal is unavailable for public inspection. However, we have neither the authority, nor the expertise, nor the inclination to overrule classification decisions made by the relevant executive branch agencies. We respect the need for such classification of sensitive national security information, and appreciate the cooperation of the agencies in the effort to limit the need for modifications and redactions.

> questions today because we are satisfied that, to the extent such accidental collection occurred in this case, any information thus acquired did not taint the investigation or prosecution of Hasbajrami.
>
> *Third*, querying databases of stored information derived from Section 702-acquired surveillance also raises novel and difficult questions. Querying, depending on the particulars of a given case (such as what databases are queried, for what purpose, and under what circumstances), *could* violate the Fourth Amendment, and thus require the suppression of evidence; therefore, a district court must ensure that any such querying was reasonable. But no information about any queries conducted as to Hasbajrami was provided to the district court, and the information provided to us on this subject is too sparse to reach a conclusion as to the reasonableness of any such queries conducted as to Hasbajrami.

Given these conclusions, further proceedings are necessary to determine (a) what (if any) evidence relevant to Hasbajrami was obtained by the government by querying databases, (b) whether any such querying violated the Fourth Amendment and, if so, (c) whether any such violation tainted other lawfully-collected evidence. We therefore REMAND the case to the district court for further proceedings consistent with this opinion.

BACKGROUND

This appeal concerns the legal status of evidence of Hasbajrami's electronic communications with individuals located abroad, which was collected by the

government without a warrant pursuant to the government's authority under Section 702. The background to this appeal may be easily summarized: Hasbajrami sought to suppress evidence the government acquired under Section 702, arguing that the government had violated his Fourth Amendment rights when it seized his communications without a warrant, and that those communications, and any information that the government later collected as the fruit of that initial warrantless surveillance, should therefore be suppressed. The district court declined to suppress the evidence, and Hasbajrami pleaded guilty while reserving his right to appeal the district court's decision.

But our disposition of the case turns in part on the particulars of how Section 702-acquired surveillance was used in Hasbajrami's prosecution; a fuller accounting of the facts of Hasbajrami's case and the nature of Section 702 surveillance is therefore necessary. First, we begin by describing Hasbajrami's arrest and the initial proceedings in which he pleaded guilty, the subsequent disclosure of Section 702 surveillance, Hasbajrami's withdrawal of his guilty plea, and his subsequent motion to suppress. Second, we describe in broad terms the operation of Section 702 surveillance. Third, we turn to the district court's discussion of the use of Section 702 evidence (that it was aware of) in this case,

and its denial of the suppression motion. Finally, we describe the proceedings at the district court following its denial of the suppression motion, and the proceedings on appeal.

I. Allegations and Initial Proceedings

The conduct underlying Hasbajrami's prosecution occurred primarily between April and August, 2011. During that time, Hasbajrami communicated by e-mail with "Individual #1," a non-American located abroad, who Hasbajrami believed was associated with a terrorist organization. In those e-mails, Hasbajrami discussed his interest in the group's terrorist operations, and Individual #1 instructed Hasbajrami how he could smuggle himself into Pakistan to join the organization. Individual #1 also detailed means by which Hasbajrami could send money to him and how Hasbajrami could contact him once he reached Pakistan. In discussing his plans to join Individual #1 in Pakistan, Hasbajrami also described his arrangements for traveling to Turkey, and his concern that his projected route from there to Pakistan might have been compromised.

Following an investigation by the agents of the Federal Bureau of Investigation's Joint Terrorism Task Force, Hasbajrami was arrested as he was

about to board a flight to Istanbul, Turkey. His luggage contained a tent, boots, and cold-weather gear. Upon arrest, Hasbajrami made certain inculpatory statements.

A. Initial Proceedings

Hasbajrami was indicted on September 8, 2011, and charged with one count of providing material support to terrorist organizations. At the same time, and as required by statute, the government gave notice that it "intend[ed] to offer into evidence, or otherwise use or disclose in any proceedings . . . information obtained or derived from electronic surveillance and physical searches conducted pursuant to [FISA]." *See* Notice of Intent to Use Foreign Intelligence Surveillance Act Information, *United States v. Hasbajrami*, 1:11-cr-623 (E.D.N.Y. filed Sept. 13, 2011), ECF No. 9.

In discovery, Hasbajrami was provided with evidence of his communications obtained pursuant to traditional FISA warrants,[2] and he

[2] As detailed below, this opinion will use "traditional FISA" to describe FISA surveillance that was authorized by statute prior to the enactment of Section 702. The FISA Amendments Act will be referred to as the "FAA," of which Section 702 is one part.

eventually pleaded guilty on April 12, 2012, to one count of providing material support to terrorists. He was sentenced to 180 months' imprisonment.

B. Disclosure of Section 702 Surveillance, Withdrawal of Plea, and Motion to Suppress

After Hasbajrami's initial plea and sentencing, and while Hasbajrami was serving his sentence, the government disclosed that it had collected Hasbajrami's communications under Section 702 of the FAA.[3] In a letter sent to Hasbajrami in February 2014, the government stated that "based on a recent determination," it had concluded that the information obtained from FISA surveillance that the government had already disclosed "was itself also derived from other collection pursuant to Title VII of FISA [*i.e.*, Section 702] as to which you were aggrieved." App'x at 31. The government stated that "certain evidence and information . . . that the government intended to offer into evidence or otherwise use or disclose

[3] The government's provision of notice in this case was likely in response the Solicitor General's assertion, at oral argument before the Supreme Court in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013), that prosecutors would provide notice to defendants in cases where evidence was derived from Section 702 surveillance. *See* Charlie Savage, *Door May Open Challenge to Secret Wiretaps*, N.Y.Times (Oct. 17, 2013), at A3. While the government's policy prior to *Clapper* was not to provide notice of Section 702 surveillance, it began reviewing cases and providing supplemental notice in 2013. *Id.*

in proceedings in this case was derived from acquisition of foreign intelligence information conducted pursuant to the FAA." *Id.*

In response to that disclosure, Hasbajrami sought leave to withdraw his plea. The district court granted that motion, finding that Hasbajrami had "specifically asked [his counsel] about whether warrantless wiretaps had played a role in his case. After [counsel] informed him that such wiretaps were not part of the evidence, he was more willing to plead guilty. Thus, Hasbajrami seems to have been misled about a fact he considered important in deciding how to plead." App'x at 39. Furthermore, the government's misleading notice, according to the district court, prevented Hasbajrami from knowing that he could challenge the evidence against him on the grounds that Section 702 was unconstitutional. The court concluded that, prior to the letter disclosing Section 702 surveillance, Hasbajrami "was not sufficiently informed about the facts" to have "made an intelligent decision about whether to plead guilty[.] When the government provided FISA notice without FAA notice, Hasbajrami was misled about an important aspect of his case." App'x at 38. Accordingly, the court allowed him to withdraw the plea and reopened the case.

Hasbajrami then moved to suppress "the fruits of all warrantless FAA surveillance," the motion that is at issue in this appeal. *See* Omnibus Motions at 8-9, *United States v. Hasbajrami*, 1:11-cr-623 (E.D.N.Y. filed Nov. 26, 2014), ECF No. 92 ("Suppression Motion"). He described what he sought to suppress, "the fruits of all warrantless FAA surveillance," as including:

- all evidence and information derived as a result of Title VII warrantless FAA surveillance;
- all evidence and information "obtained or derived from Title I and Title III FISA collection . . . [that was] itself also derived from other collection pursuant to Title VII" of the FAA;
- Hasbajrami's custodial statements; and
- Any other evidence and information that the Government could not have obtained in this case through an independent source.

Id.

To properly understand the scope of Hasbajrami's motion, however, it is necessary to describe the statutory framework underpinning Section 702 surveillance and the way in which the program operates in practice.

II. Section 702 Surveillance[4]

In order to ensure national security, the United States maintains several programs aimed at the surveillance of those who pose threats to its safety. These programs each draw on a wide variety of authority, including executive orders, statutory provisions, and agency procedures and guidance. *See generally* Diana Lee, Paulina Perlin & Joe Schottenfeld, *Gathering Intelligence: Drifting Meaning and*

---

[4] The purpose of this section is to provide the general background necessary to understand the parties' arguments and it is not intended to provide a comprehensive description of the way in which each agency implements Section 702 surveillance. Additionally, as detailed below, each agency must seek approval of its Section 702 procedures each year, including changes in operation. Our intention is thus only to describe the program in broad terms. We note, moreover, that many Section 702 procedures remain highly classified, including the specific procedures under which the collection of Hasbajrami's communications would likely have taken place. Our discussion here is drawn from declassified public sources and in large part from the report on Section 702 surveillance produced by the Privacy and Civil Liberties Oversight Board. *See* Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (July 2, 2014), https://www.pclob.gov/library/702-Report.pdf ("PCLOB Report"). The PCLOB is an independent agency within the executive branch, authorized by statute, *inter alia*, to "analyze and review actions the executive branch takes" and "ensure that liberty concerns are appropriately considered" in the government's development and implementation of anti-terrorism programs. *See* 42 U.S.C. § 2000ee(c). The PCLOB is composed of five members, appointed by the President and confirmed by the Senate. *Id.* § 2000ee(h).

Accordingly, we discuss the program, and changes in its operation over time, only to the extent that the details are (a) relevant and (b) public.

the Modern Surveillance Apparatus, 10 J. of Nat'l Sec. L. & Pol'y 77 (2019) (describing several separate authorities for surveillance, including FISA and Section 702, each with separate operating standards). Hasbajrami's appeal specifically implicates the government's statutory authority under FISA, first enacted in 1978, and more specifically the amendments to FISA, including Section 702, enacted in 2008.[5]

FISA was first enacted in response to revelations about the government's electronic surveillance of the domestic communications of United States citizens. *See* David S. Kris & J. Douglas Wilson, National Security Investigations and Prosecutions § 3:7 ("Kris & Wilson"). "Traditional FISA" surveillance, as surveillance under the FISA has come to be known following the enactment of the FAA in 2008, governed surveillance inside the United States, in the context only of national security investigations rather than domestic criminal prosecutions. *See id.* § 4:2. For those national security investigations, FISA established procedures governing the collection of information derived from

[5] While Section 702 was first enacted in 2008, the fact that any e-mails tied to Americans were sometimes collected under its authority was not made public until June 2013, when "two classified [National Security Agency ("NSA")] collection programs were first reported by the press based on unauthorized disclosures of classified documents by Edward Snowden, a contractor for the NSA." PCLOB Report at 1.

electronic surveillance, physical searches, "pen/trap" surveillance, and tangible-things production orders, and the use of information so obtained. *See id.* § 4:5.

In order to initiate traditional FISA surveillance, the government must submit an application to a court demonstrating that there is "probable cause to believe that 'the target of the electronic surveillance is a foreign power or agent of a foreign power,' and that each of the specific 'facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power.'" *See Clapper*, 568 U.S. at 403 (quoting FISA § 105(a)(3)). FISA applications are reviewed by two specialized courts: the Foreign Intelligence Surveillance Court ("FISC") and the Foreign Intelligence Surveillance Court of Review ("FISCR"), both composed of Article III federal judges assigned to their role by the Chief Justice of the United States. *See id.*; Kris & Wilson § 5:1 (describing jurisdiction of FISC and FISCR). Applications are submitted under oath by a federal officer and must describe, among other things, whom the government wishes to search or surveil, the place or things to be searched or surveilled, the sort of information the government expects to gather, and the existence and nature of any prior FISA applications targeting the individual. *See generally* Kris & Wilson § 6:2.

Traditional FISA had some limitations, however. Because each application required a court order, which in turn required probable cause, the government believed "that, after September 11, 2001, [FISA's] requirements unduly restrict[ed the] speed and agility" with which the government could detect and respond to terrorist threats. *See id.* § 16:2 (internal quotation marks omitted). Additionally, the advent of e-mail "clearly expanded traditional FISA's reach." *Id.* § 16:6. Communications, such as phone calls, between two individuals without ties to the United States and located abroad were outside the purview of FISA, and any collection of such communications that occurred would not be constrained by its procedures. *Id.* But as such communication increasingly came to be conducted by e-mail, many of those e-mails would ultimately be stored on servers within the United States, and thus "the government could not conduct warrantless surveillance in the U.S. of stored e-mail messages exchanged between two parties located abroad" without following the procedures laid out in FISA. *Id.*

First enacted in 2008, Section 702 was intended to address some of FISA's perceived limitations.[6] Section 702 allows the Attorney General ("AG") and

[6] President George W. Bush initially authorized the NSA "to conduct warrantless wiretapping of telephone and e-mail communications where one party to the communication was located outside the United States" and one party was believed to be a member of a terrorist organization. *See Clapper,* 568 U.S. at 403.

Director of National Intelligence ("DNI") to "authorize jointly . . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 1881a(a).[7] That targeting is primarily executed by compelling electronic service providers, including internet service providers and companies that maintain the communications infrastructure, to "immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition [of communications of an individual or his or her account] in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such electronic communication service provider is providing to the target of the acquisition." 50 U.S.C. § 1881a(i)(1)(A).

Following public revelations of the program, Congress passed the Protect America Act ("PAA"), Pub. L. No. 110-55, 121 Stat. 552 (2007), which for a limited period of time allowed the government to use surveillance procedures similar to those contained in the FAA. *See In re Directives*, 551 F.3d 1004, 1006-07 (FISA Ct. Rev. 2008). The PAA expired on February 16, 2008. *See id.* at 1006 n.1.

[7] Like other sections of the FISA, Section 702's definition of "United States person" includes lawful permanent residents (such as Hasbajrami). *See* 50 U.S.C. § 1801(i) (defining "United States person" to be a "citizen of the United States, an alien lawfully admitted for permanent residence" or certain unincorporated associations or corporations with ties to the United States).

Section 702 differs from traditional FISA procedures in several key respects. First, Section 702 does not require a probable cause determination before undertaking surveillance. *Clapper*, 568 U.S. at 404. Second, Section 702 "does not require the Government to specify [in a FISA application] the nature and location of each of the particular facilities or places at which the electronic surveillance will occur." *Id.* Instead, as detailed below, the FISC approves Section 702 procedures in advance, targeting non-United States persons located abroad as a category, and the government does not have to return to the FISC to seek approval before it undertakes surveillance of any specific individual or his or her accounts under those Section 702 procedures. *See* Kris & Wilson § 17:17.

In short, under the FAA and Section 702 the government may compel service providers located in the United States to provide e-mails or other electronic communications to, from, or about individuals the government believes are (a) not United States persons and (b) located abroad.[8] Both under the

[8] The FAA also contains two sections, Sections 703 and 704, that address the direct targeting of individual United States persons outside the United States for electronic surveillance. *See* Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 Harv. J.L. & Pub. Pol'y 117, 142-44 (2015). The procedures followed "generally reflect the structure employed by traditional FISA with regard to electronic surveillance and physical search." *Id.* at 143. These sections are codified at 50 U.S.C. §§ 1881b and 1881c, and are not at issue in this appeal.

statutory scheme and in practice, Section 702 surveillance unfolds in several different steps, each with different implications for this Court's review. The first step is what the statute and intelligence community refers to as "targeting," followed by collection, "minimization," retention and storage, and, finally, dissemination and querying.[9] We will discuss each step in turn.

A. "Targeting"

Targeting generally refers to the decision to surveil an individual or his or her channels of electronic communications, such as an e-mail address. The government may not "intentionally target" for Section 702 surveillance anyone located in the United States or a "United States person" outside the United States. 50 U.S.C. §§ 1881a(b)(1), (3). Nor may it target a non-United States person "if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States." 50 U.S.C. § 1881a(b)(2).

---

[9] Some of these terms, such as collection, are terms of art, but their use is not necessarily uniform across the various government agencies or for different forms of surveillance. *See, e.g.*, Lee, Perlin & Schottenfeld, *Gathering Intelligence* at 95 (highlighting "definitional variances" for terms like collection, acquisition, and targeting across the various surveillance programs). For the purposes of providing background to Hasbajrami's case, we define the terms primarily as each is used by the PCLOB.

The precise mechanisms each agency must follow to target communications are not specified by the statute. Instead, Section 702 requires the AG and the DNI to adopt targeting procedures each year that will govern how the program functions at each agency tasked with Section 702 surveillance. *See* 50 U.S.C. §§ 1881a(a), (d). While labelled targeting procedures, the procedures are just as much about who *is not* to be targeted under Section 702 (that is, how to prevent acquisition of the communications of those in the United States or who are United States persons) as about setting out who *is* to be targeted. In this opinion, our concern with "targeting" is with the procedures designed to protect the constitutional privacy rights of Americans and comply with the Fourth Amendment inside the United States, and not with the obviously confidential procedures and criteria by which United States intelligence agencies decide which non-United States persons located abroad are appropriate objects of surveillance.

The targeting procedures are supposed to ensure that any authorized acquisition is "limited to targeting persons reasonably believed to be located outside the United States" and to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at

the time of the acquisition to be located in the United States." 50 U.S.C. § 1881a(d)(1). Targeting procedures are also subject to the limitations related to targeting United States persons outlined above. 50 U.S.C. § 1881a(b). The NSA and the FBI each develop targeting procedures tailored to the agency's particular mission and purpose in using Section 702-acquired information. PCLOB Report at 41-43, 47.

Once the required procedures have been formulated, the DNI and AG must seek approval of their proposed targeting procedures from the FISC. 50 U.S.C. § 1881a(d)(2). The FISC reviews the proposed standards for compliance with both statutory and constitutional requirements. *See, e.g., In re Proceedings Required by 702(i) of FISA Amendments Act of 2008*, No. MISC 08-01, 2008 WL 9487946, at *5 (FISA Ct. Aug 27, 2008); *Redacted*, 2011 WL 10945618 at *1 (FISA Ct. Oct. 3, 2011) ("*Bates Decision*"). In contrast to traditional domestic search warrants and FISA warrants, which authorize searches or seizures of specific persons, places, or things based on individualized probable cause, judicial review of Section 702 functions as a form of programmatic pre-clearance. "[T]he Court is required to consider whether the targeting . . . procedures adopted by the Government meet the requirements of the statute and . . . are consistent with

the Fourth Amendment. The Court is not required, in the course of this Section 702(i) review, to reach beyond the Government's procedures and conduct a facial review of the constitutionality of the statute." *In re Proceedings*, 2008 WL 9487946, at *5; *see also* PCLOB at 26-31 (describing judicial review proceedings under Section 702).

Once its procedures are approved by the FISC, an agency can begin surveilling individuals it seeks to target. The NSA "initiates all Section 702 targeting, and thus makes all initial decisions pursuant to its targeting procedures." PCLOB Report at 42. According to the PCLOB, the CIA and the FBI can "'nominate' targets to the NSA for Section 702 targeting" but the NSA is required to "make the determination whether to initiate targeting." *Id.*

Section 702 surveillance usually begins when an agency "tasks" a specific "selector" or "facility," usually an e-mail address or telephone number. *See id.* at 32. Much information about the targeting standards used by the NSA remains classified, but generally "[i]f they are to fulfill their purposes . . . [the targeting procedures submitted to the FISC for approval] should contain a description of factors that in isolation or combination justify a reasonable belief that the target is abroad." Kris & Wilson § 17:7. According to one commentator, the NSA "has

created a presumption of non-U.S. person status," assuming "that the individual is a non-U.S. person" if the agency does not know its target is a United States person. *See* Donohue, *Section 702* at 158.

B. Collection

Once an account or facility such as an e-mail address has been targeted, the intelligence agencies may then begin to collect information related to that particular address. Such information includes e-mails to and from a given account, or information "about" a given account.

1. PRISM and Upstream Collection

The NSA operates two separate types of collection programs which collect different types of information. These two programs have come to be labelled *PRISM collection and upstream collection.*

Under PRISM, the FBI (on behalf of the NSA) sends "selectors" (for instance, an e-mail address) to internet service providers ("ISPs"), based in the United States. The ISPs are then required to provide communications sent to or from that selector to the NSA. *See* PCLOB Report at 33-34. PRISM, therefore, collects only the e-mails a given user sends from his or her account, and the e-mails he or she receives from others through that account. *Id.* at 34. Collection

and review of such material happens roughly in real time, or close to real time. In other words, the collected e-mails are not simply swept into a database for use at some unspecified future time when the database is queried, but are monitored and analyzed at or near the time of their collection. In that regard, the interception and review of electronic communications under PRISM resembles a traditional domestic law enforcement wiretap.

Upstream collection is broader. Instead of compelling information from an ISP, the NSA instead compels information from "the providers that control the telecommunications backbone over which communications transit." PCLOB Report at 35. Upstream fills a gap in PRISM surveillance. *Id.* If, for instance, an individual that the NSA sought to target maintained his or her e-mail account with a foreign internet service provider, that e-mail address would be out of reach of the PRISM program. In that situation, the NSA could use upstream collection to collect traffic to that account as it traversed the backbone. *Id.* Upstream collection is broader than PRISM, in that it captures not only conversations to and from a given e-mail address, but also communications "about" that address (*i.e.*, a conversation between two parties not themselves targeted that happens to mention whatever the tasked term is). *See id.* at 37-38.

One key difference between PRISM and upstream collection is that PRISM collects individual communications, while upstream collects whole "multi-communication transactions," or "MCTs." *Id.* at 39. "An Internet transaction refers to any set of data that travels across the Internet together such that it may be understood by a device on the Internet." *Id.* Thus, a transaction might contain a single discrete communication (*e.g.*, a single e-mail), or it could contain "multiple discrete communications," and "[i]f a single discrete communication within an MCT is to, from, or about a Section 702-tasked selector, and at least one end of the transaction is foreign, the NSA will acquire the entire MCT" under upstream collection. *Id.* The result is a "greater likelihood" that upstream collection will "result in the acquisition of wholly domestic communications and extraneous U.S. person information." *Id.* at 41. The NSA is the only agency that receives upstream collection; the CIA and FBI are not provided with information obtained in this manner and do not store it in their databases. *Id.* at 54.

2. Incidental and Inadvertent Collection

As detailed above, the statute primarily authorizes agencies like the NSA to collect the e-mails of "non-United States persons" located abroad. But even if the government scrupulously follows the procedures intended to restrict

collection of communications to and from persons with ties to the United States, the agencies might still end up collecting information about United States persons or those located in the United States, or communications sent to or from a United States person or an individual located in the United States.

Collection may sweep up those individuals' e-mails in two ways, conventionally referred to as "incidental collection" and "inadvertent collection." First, collection might be "incidental." PCLOB Report at 114. Incidental collection occurs when a non-targeted individual (a United States person or someone in the United States) communicates with a targeted non-United States person located abroad. Such collection would occur under PRISM, for instance, if the NSA has targeted the e-mail address of a non-United States person in another country, and a United States person e-mails that targeted individual. An ISP would be required to provide the NSA with any such e-mails as part of its compliance with a Section 702 directive targeting the non-United States party to the communication.

Second, collection might be "inadvertent." *Id.* at 116. Inadvertent collection occurs when the NSA reasonably believes that it is targeting a non-United States person located abroad, or does not have enough information to determine

whether an individual e-mail address or other communications facility is being used by a United States person or accessed from within the United States, and therefore presumes that the account is controlled by a foreigner outside the United States. The collection is characterized as "inadvertent" when the agency learns that the person controlling the account is a United States person after it has already acquired some of the person's communications. In essence, *inadvertent collection occurs when* the NSA targets United States persons or individuals located within the United States in error: the agency thought it was targeting a foreign individual abroad, but the targeted person was in fact a United States person or an individual located in the United States.

C. "Minimization"

In general terms, minimization describes the manner in which the government processes communications after they have been collected and seeks *to provide safeguards against the* misuse of Section 702 information. *See* PCLOB Report at 50. The 2011 Minimization Procedures, which have been declassified, apply "to the acquisition, retention, use, and dissemination of non-publicly available information concerning unconsenting United States persons that is acquired by targeting non-United States persons reasonably believed to be

located outside the United States." *See Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended* § 1, National Security Agency (Oct. 31, 2011), https://www.dni.gov/files/documents/Minimization%20Procedures%20Used%20By%20NSA%20In%20Connection%20With%20FISA%20Section%20702.pdf ("NSA 2011 Minimization Procedures").[10]

As with their targeting procedures, the NSA, FBI, and CIA must seek yearly approval of their minimization procedures from the FISC. 50 U.S.C. § 1881a(e)(2). Section 702 requires that each agency also adopt procedures that prohibit the disclosure of information about United States persons in a manner that identifies them, unless that identity is necessary to understand the intelligence information. *See* 50 U.S.C. § 1881a(e)(1) (cross-referencing 50 U.S.C. §§ 1821(4) and 1801(h)); *see also* Kris & Wilson § 9:1. By statute, the procedures must ensure "that nonpublicly available information, which is not foreign intelligence information . . . shall not be disseminated in a manner that identifies

[10] These minimization procedures were submitted to the FISC for approval after Hasbajrami's arrest, and therefore did not govern the operation of Section 702 during the time period relevant here.

any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance." 50 U.S.C. § 1801(h)(2).

Minimization procedures seek to "balance the government's need to acquire, retain, and disseminate foreign intelligence information, against the countervailing privacy interests of U.S. persons." Kris & Wilson § 9:1; PCLOB Report at 50 ("*Minimization procedures are best understood as a set of controls* on data to balance privacy and national security interests."). The meaning of the term as used in the FISA context is subtly different from what it means in the more familiar context of court-authorized domestic electronic surveillance by law enforcement agencies under traditional domestic wiretaps. In the latter context, minimization procedures generally involve stopping the monitoring of communications that can be determined in real time to be non-evidentiary. In the context of Section 702 surveillance, the information subject to minimization has already been collected. After review, it is either retained or destroyed; information is "minimized" by non-retention. NSA analysts are instructed to "exercise reasonable judgment in determining whether information acquired must be minimized and will destroy inadvertently acquired communications of

or concerning a United States person at the earliest practicable point in the processing cycle at which such communication can be identified either: as clearly not relevant to the authorized purpose of the acquisition (e.g., the communication does not contain foreign intelligence information); or, as not containing evidence of a crime which may be disseminated under these procedures."[11] NSA 2011 Minimization Procedure § 3(b)(1).

After an NSA analyst reviews an individual e-mail communication, he or she will decide if the information warrants retention in the NSA's databases and/or dissemination to other agencies. The analyst will determine if "it is a domestic or foreign communication to, from, or about a target and is reasonably believed to contain foreign intelligence information or evidence of a crime." *Id.* § 3(b)(4). Communications fitting this description will thus be retained and processed; information not involving foreign intelligence information or evidence of a crime will be destroyed unless it meets one of several exceptions,

[11] It is not clear whether the minimization procedures' use of "inadvertent" here is intended broadly to invoke the word's plain meaning, or is used as a term of art to apply the provision only to communications acquired as a result of "inadvertent collection," as defined above, where a United States person has been erroneously targeted.

such as when "the communication contains information pertaining to a threat of serious harm to life or property." *Id.* § 5(4).

When an e-mail or other communication is processed and retained, the information will be scanned and stored. Information that "do[es] not meet the retention standards . . . and . . . [is] known to contain communications of or concerning United States persons" will be "destroyed upon recognition." *Id.* § 3(c)(1). If a target moves to the United States, or if the NSA uncovers information that the target is a United States person, "acquisition from that person will be terminated without delay." *Id.* § 3(d)(1).

"[D]omestic communications" — all communications that do not have "at least one communicant outside the United States," *id.* § 2(e), "will be promptly destroyed," except under certain conditions. *Id.* § 5. Such conditions include if a communication is "reasonably believed to contain significant foreign intelligence information," which may be provided to the FBI (which in turn may disseminate information "in accordance with its minimization procedures"). *Id.* § 5(1). Information that is "reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed" may be "disseminated (including

United States person identities) to appropriate Federal law enforcement agencies." *Id.* § 5(2).

D. Retention and Dissemination

As addressed above, the minimization procedures also govern the ultimate retention of surveillance materials and the "reporting of acquired information outside of [the] intelligence agency" that collects the information. PCLOB Report at 64. The minimization procedures treat retention and dissemination in similar ways: the NSA, for instance, may retain communications "in generally the same situations where the NSA is permitted to disseminate . . . these communications" to other agencies. *Id.* at 62.

The retention and dissemination of information gathered under the FAA is also governed by the same restrictions that apply to traditional FISA. *Id.* at 64. Additional protections generally apply if the NSA, for instance, seeks to disseminate Section 702 information containing the identity of a United States person. The NSA will then "mask" the identity, deleting any identifying information unless certain exceptions apply. These exceptions include when "the U.S. person's identity is necessary to understand foreign intelligence

information, or the communication contains evidence of a crime and is being disseminated to law enforcement authorities." *Id.* at 65.

Agencies relying on NSA reporting may request that the identity of a United States person be unmasked. *Id.* The NSA may provide that information if at least one additional criterion is met, including when "the identity of the United States person is necessary to understand foreign intelligence information" or the information "indicates that the United States person" is an "agent of a foreign power" or the "target of intelligence activities of a foreign power." NSA 2011 Minimization Procedure § 6(b). Agencies may also request that information about a given e-mail address or facility be forwarded on a regular basis.

E. Storage and Querying

Once communications are collected and retained or disseminated, each agency may establish databases to store those communications in its possession, and may query those stored communications to identify information of interest in connection with a particular investigation or agency function.

The NSA, CIA, and FBI each maintain separate databases containing Section 702 information on which the agencies rely for their own purposes. PCLOB Report at 55-56. According to the PCLOB, the NSA, for instance, "often

stores data acquired from multiple legal authorities in a single data repository." PCLOB at 55. The agency then "tags" the sources for each piece of information, and "has systems that prevent an analyst from accessing or querying data acquired under a legal authority for which the analyst does not have the requisite training."[12] *Id.* at 55-56. The CIA limits access to databases that contain Section 702-acquired information to only those agents who have had the requisite training. *Id.* at 55. And the FBI "stores electronic data obtained from traditional FISA electronic surveillance and physical searches . . . in the same repositories as the FBI stores Section 702-acquired data." *Id.* at 59. An agent without requisite training would see whether a piece of Section 702-acquired information was responsive to her query, but she would not be able to view the actual underlying material without clearance. *Id.*

"Data is frequently reviewed through queries, which identify communications that have particular characteristics specified in the query, such as containing a particular name or having been sent to or from a particular e-mail address." *Id.* at 127. Colloquially, the parties (and those engaged in policy

[12] Each agency with access to Section 702 data provides training to personnel regarding the proper use of Section 702 material, as well as the agency's minimization procedures. *See* PCLOB Report at 53-54. The exact training procedures and who is trained may vary by agency.

debates about the program) have referred to this querying capability as "backdoor searches."

Originally, the minimization procedures precluded analysts from searching terms associated with United States persons. *See* Classified Supplemental App'x at 121-22 ([redacted] In April 2011, the government sought approval for new minimization procedures that allowed the querying of terms related to United States persons. *See Bates Decision*, 2011 WL 10945618 at *7-8. The FISC ultimately approved the new procedures in October 2011 (*i.e.*, after Hasbajrami's arrest) because they were "designed to yield foreign intelligence information." *Id.* at *7. Querying, the court stated, "should not be problematic in a collection that is focused on non-United States persons located outside the United States and that, in the aggregate, is less

likely to result in the acquisition of nonpublic information regarding non-consenting United States persons." *Id.*

In a June 2014 letter to Senator Wyden, Deirdre Walsh, Director of Legislative Affairs for the Office of the Director of National Intelligence, stated that each of the three agencies allowed querying. The NSA could query Section 702-acquired information if it had a "reasonable basis to expect the query will return foreign intelligence," as could the CIA and the FBI. *See* Response to Question from the 5 June 2014 Hearing, Letter from Deirdre Walsh, Director of Legislative Affairs, to Senator Ron Wyden (June 27, 2014) ("Walsh Letter"); *see also* PCLOB Report at 57-58. The FBI is also allowed to query its own databases in such a way that these queries are "designed to find and extract evidence of a crime." Walsh Letter at 2. The FBI also will query previously acquired information from a variety of sources, including Section 702 when it "opens new national security investigations." *Id.* at 3.

Recently, and after the time period at issue in this case, Congress enacted the FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, 132 Stat. 3 (2018), codified at 50 U.S.C. § 1881a. The act amended the FAA to require the agencies to develop "querying procedures" alongside their targeting and

minimization procedures and seek approval of all three sets of procedures yearly from the FISC. Congress also amended the FAA to require a court order in most cases where the FBI seeks to "access the contents of communications . . . that were retrieved pursuant to a query made using a United States person query term that was not designed to find and extract foreign intelligence information." 50 U.S.C. § 1881a(f)(2)(A). Such querying standards were not in place when the surveillance at issue here occurred.

III. The District Court's Denial of Hasbajrami's Suppression Motion

As noted above, Hasbajrami moved to suppress "the fruits of all warrantless FAA surveillance." *See* Suppression Motion at 8. He also moved for discovery of the FISA and Section 702 information relevant to his case.

After the district court reviewed the relevant materials *ex parte* and *in camera*, it denied the suppression motion. *See United States v. Hasbajrami*, 1:11-cr-623, 2016 WL 1029500 (E.D.N.Y. Feb. 18, 2016) ("*Suppression Decision*").[13] It treated the suppression motion as an as-applied challenge to the Section 702 surveillance used to support the government's initial application to the FISC,

[13] As addressed below, the district court announced its decision on February 15, 2015, in a text order on the docket, issued without an opinion. The redacted opinion was issued on the public docket in March 2016.

primarily addressing the issue of collection. *Id.* at *7. First, after noting the distinction between PRISM and upstream collection, the court concluded that "[n]one of the Section 702 communications used in Title I and Title II FISA applications targeting the agent of the foreign power were 'about' communications" and therefore "the constitutionality of upstream collection [was] not at issue" in Hasbajrami's case. *Id.* at *6-7.

The district court then turned to PRISM collection. Summarizing precedent, the court noted that the Fourth Amendment "does not constrain the government from collecting the communications of non-U.S. individuals targeted by Section 702 surveillance." *Id.* at *7. Although Hasbajrami was a legal permanent resident located in the United States, the court found that it was "non-U.S. persons who were the targets of Section 702 surveillance" and that Hasbajrami's e-mails were collected incidentally to the surveillance of individuals the court described as "legitimate targets of Section 702 surveillance." *Id.* The court concluded that the incidental interception of the communications of individuals in the United States was constitutional because the surveillance was "lawful in the first place — whether it is the domestic surveillance of U.S. persons pursuant to a warrant or the warrantless surveillance

of non-U.S. persons who are abroad — [and therefore] the incidental interception of non-targeted U.S. persons' communications with the targeted persons is also lawful." *Id.* at *9.

The court did not address whether any inadvertent collection related to Hasbajrami. It also did not address the specifics of any querying as applied to Hasbajrami in particular, and there does not appear to have been any fact-finding regarding the querying of previously-collected communications with identifiers related to Hasbajrami. Instead, the parties had raised querying within the context of whether the minimization procedures were reasonable, and the government argued that it was permitted to query whatever data it had lawfully collected *even if* it used identifiers it knew were associated with United States persons. *See* Gov't Mem. of Law at 71, *United States v. Hasbajrami*, 1:11-cr-623 (E.D.N.Y. filed Dec. 23, 2014), ECF No. 97. To the extent that the district court considered querying, then, it appeared to adopt the government's position, stating in a footnote:

> That the government is able to query information obtained under the PRISM program, *i.e.* lawfully-obtained communications that were to or from legitimate targets, does not render the minimization procedures inadequate, as *amici* contend . . . . Here, once the government learned that the target was potentially

> an agent of a foreign power, the government sought orders from the FISC for electronic surveillance and physical searches pursuant to Title I and Title III of FISA targeting an agent of a foreign power. . . . I agree with the government that "[i]t would be perverse to authorize the unrestricted review of lawfully collected information but then [] restrict the targeted review of the same information in response to tailored inquiries." Gov't Br. at 71-72.

Suppression Decision, 2016 WL 1029500 at *12 n.20.

As for Hasbajrami's request to provide discovery to properly-cleared defense counsel, the district court concluded that disclosure was unnecessary. *Id.* at *14. Instead, its review was "relatively straightforward and not complex" and the district court was "able to evaluate the legality of the challenged surveillance without concluding that due process first warranted disclosure." *Id.* at *14 (citing *United States v. Abu-Jihaad*, 630 F.3d 102, 129 (2d Cir. 2010)).

IV. Further Proceedings at the District Court

The district court denied the motion to suppress in a text order dated February 20, 2015. The order stated that "[a]n opinion [would] follow," but that the motion would be denied as to "the fruits of the FAA surveillance, including the defendant's post-arrest statements." App'x at 16. The court noted that it would hold a conference and "inquire of the government whether it intends to offer once again the charge bargain that was previously accepted by the

defendant, and whether it has considered the prospect of allowing the defendant to enter such a plea pursuant to Rule 11(a)(2), reserving his right to seek appellate review of [the district court's] denial of the motion to suppress evidence." *Id.*

The parties prepared for trial, but Hasbajrami in due course again pleaded guilty, this time to a two-count Superseding Information, which charged him with providing and attempting to provide material support to terrorists. According to the terms of the agreement, Hasbajrami:

> [A]gree[d] not to file an appeal or otherwise challenge . . . the conviction or sentence in the event that the Court imposes a term of imprisonment of 180 months or below, with the sole and limited exception that, pursuant to Federal Rule of Criminal Procedure 11(a)(2), the defendant may appeal the District Court's February 20, 2015 denial of his motion to suppress evidence that was obtained or derived from surveillance conducted pursuant to the FISA Amendments Act of 2008, 50 U.S.C. §§ 1881a *et seq.*

App'x at 48. Hasbajrami also consented to his removal, after serving his sentence, from the United States. The district court sentenced Hasbajrami to a term of 180 months' imprisonment on Count One and 12 months' imprisonment on Count Two, each to run consecutively.

On March 8, 2016 — more than one year after it denied the motion — the district court issued a redacted opinion on the public docket explaining its reasons for denying suppression. Hasbajrami requested that the full decision be released to his cleared defense counsel, so that he might better prepare his appeal. The court (Dora L. Irizarry, *C.J.*)[14] held that FISA required redaction and that "Defendant's counsel are not entitled to view the Unredacted Opinion because releasing it would reveal classified foreign intelligence information and circumvent FISA . . . ." *United States v. Hasbajrami*, 1:11-cr-623, 2017 WL 3610595 at *3 (E.D.N.Y. April 6, 2017).

V. Proceedings on Appeal

Hasbajrami timely filed two notices of appeal. The first addressed the district court's denial of Hasbajrami's motion to suppress; the second addressed the district court's decision to deny Hasbajrami's counsel access to the unredacted and unmodified version of the suppression ruling. Both appeals were consolidated and argument was heard by this Court on August 27, 2018.

At oral argument, the government was unable to represent whether or not identifiers related to Hasbajrami had been used in querying previously-acquired

[14] By this point, the case had been transferred to Chief Judge Irizarry following Judge Gleeson's resignation.

Section 702 surveillance databases. This Court therefore ordered the government to "identify[] the record evidence that supports the proposed factual inference that it conducted no queries or backdoor searches of Section 702 material with regard to Hasbajrami before or leading to the FISA court's issuance of Title I and Title III warrants with respect to Hasbajrami." Order, *United States v. Hasbajrami*, Nos. 15-2684, 17-2669 (2d Cir. Sept. 4, 2018), ECF No. 203.

Both parties filed supplemental briefing, including an additional classified brief from the government (which was posted, heavily redacted, on the public docket for this appeal).

DISCUSSION

Hasbajrami primarily raises an as-applied challenge to the constitutionality of warrantless collection and review of his communications under Section 702.[15] As the PCLOB notes, judicial review of Section 702 surveillance presents particular challenges because the program:

> entails many separate decisions to monitor large numbers of individuals, resulting in the annual collection of hundreds of millions of communications of

[15] Hasbajrami also raises an alternative statutory argument, arguing that suppression was warranted because he claims the surveillance did not comply with the requirements of Section 702 itself. The Court has carefully considered the argument, in light of the classified record, and finds it without merit.

> different types, obtained through a variety of methods, pursuant to multiple foreign intelligence imperatives, and involving four intelligence agencies that each have their own rules governing how they may handle and use the communications that are acquired.

PCLOB Report at 86. In other words, review is difficult because we must consider those individual "separate decisions" within the context of the program as a whole.[16]

In this case, it is undisputed that the government possessed ample evidence obtained from surveillance authorized by a FISA warrant to convict Hasbajrami. The evidence that formed the basis for that warrant, however, was obtained as a result of warrantless Section 702 surveillance of non-United States persons located abroad. Thus, the primary issue, affecting the bulk of the evidence against Hasbajrami, is whether the incidental collection of the communications of United States persons, without a warrant, violates the Fourth Amendment. We conclude, as did the district court, that such collection is lawful. But that is not the only action involving Section 702 surveillance at issue here.

---

[16] When reviewing a district court's denial of a motion to suppress evidence, we review the court's legal determinations *de novo* and its factual findings for clear error. *United States v. Boles*, 914 F.3d 95, 102 (2d Cir. 2019). The issues on appeal are legal, and therefore our review here is *de novo*.

We must also address inadvertent collection, storage and querying, as each of these issues is raised by the record.

The record is sufficient to permit us to answer the principal question before us: we conclude that the district court correctly held that the incidental collection in this case, and the government's use of the information thus collected, was lawful. The record also permits us to conclude that, even assuming that inadvertent collection of the communications of United States persons may in some circumstances violate the Constitution, the effect of any such collection in this case was harmless beyond a reasonable doubt. The absence of evidence in the record regarding [redacted], however, prevents us from determining the reasonableness of any such querying [redacted] prior to the FISC's probable-cause finding, and from fully understanding how if at all the results of such querying affected the subsequent conduct of the investigation. As a result, we must remand for further proceedings and fact-finding by the district court.

I. "Incidental" Collection

The primary type of Section 702 collection we must address here involves "incidental" collection. The government was "targeting," within the meaning of Section 702, the accounts of individuals located abroad who were reasonably believed to be agents of terrorist organizations. In collecting communications from those accounts, the government collected e-mails between Hasbajrami and [redacted] In reviewing Hasbajrami's suppression motion, the district court focused on this incidental collection, ultimately concluding that a warrant was not required and the government's actions were reasonable.

On appeal, Hasbajrami and the *amici* argue that the Fourth Amendment bars the incidental collection of e-mails of individuals, like Hasbajrami, located in

the United States. First, they argue that surveillance of individuals in the United States is *per se* unreasonable if it is conducted without a warrant. They also focus on the specific attributes of warrants — the particularity requirement, the need for a neutral judicial forum and a finding of probable cause — and argue that Section 702, the targeting and minimization procedures, and FISC oversight do not provide a substitute procedure *sufficient* to satisfy the Fourth Amendment. According to Hasbajrami, the broad scope of Section 702's surveillance and the government's failure to seek a warrant or its equivalent render the program unconstitutional as applied to him and therefore requires the suppression of evidence acquired under the program.

We disagree. In addressing the issues before us, we adopt an approach similar to that employed by the United States Court of Appeals for the Ninth Circuit in *United States v. Mohamud*, 843 F.3d 420 (9th Cir. 2016). We must first decide whether a warrant is required for the government's incidental collection of the communications of United States persons. We conclude that a warrant is not required for such collection. But "[e]ven if a warrant is not required, a search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution." *Maryland v. King*, 569 U.S. 435, 448 (2013); *see also*

Mohamud, 843 F.3d at 441. We further conclude that the incidental collection of Hasbajrami's e-mails was reasonable.

A. No Warrant was Required

We conclude that a warrant is not required based on two well-established principles of Fourth Amendment law. First, the Fourth Amendment does not apply extraterritorially to the surveillance of persons abroad, including United States citizens. Second, law enforcement officers do not need to seek an *additional* warrant or probable cause determination to continue surveillance when, in the course of executing a warrant or engaging in other lawful search activities, they come upon evidence of other criminal activity outside the scope of the warrant or the rationale justifying the search, or the participation of individuals not the subject of that initial warrant or search.

First, the Fourth Amendment (and, in particular, its warrant requirement) does not apply extraterritorially. *See United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990). In *Verdugo-Urquidez*, agents from the United States Drug Enforcement Agency, working alongside Mexican law enforcement, raided without a warrant properties in Mexico owned by the defendant. *Id.* at 262–63. The agents believed that the defendant was the leader of a narcotics smuggling ring and they seized

documents and "a tally sheet" detailing quantities of drugs possessed and transported. *Id.* Prior to trial, the defendant sought suppression of the evidence, arguing that the agents should have sought a warrant before searching his property. *Id.* at 263-64.

The Supreme Court held that suppression of the evidence was not required, because the Fourth Amendment does not apply to extraterritorial actions by law enforcement, at least where the "[the defendant] was a citizen and resident of Mexico with no voluntary attachment to the United States, and the place searched was located in Mexico." *Id.* at 274-75. "Under these circumstances," the Court held, "the Fourth Amendment ha[d] no application." *Id.* at 275.

This Court has since extended *Verdugo-Urquidez*'s holding to conclude that the Warrant Clause of the Fourth Amendment does not apply to the surveillance of United States citizens abroad. *See In re Terrorist Bombings*, 552 F.3d 157, 171 (2d Cir. 2008). The defendant in that case, a United States citizen with a home in Kenya, had "urged the suppression of the evidence resulting from the . . . [electronic] surveillance of his Kenyan telephone lines" because it was not authorized by a valid warrant or, alternatively, because the surveillance was

unreasonable. *Id.* at 160. This Court held that "the Fourth Amendment's Warrant Clause has no extraterritorial application and that foreign searches of U.S. citizens conducted by U.S. agents are subject only to the Fourth Amendment's requirement of reasonableness." *Id.* at 171. We determined that the searches in that case were ultimately reasonable and therefore suppression of the evidence was not required.

Verdugo-Urquidez and *In re Terrorist Bombings* make it clear that the Fourth Amendment does not require the government to obtain a warrant before collecting the e-mails of foreign individuals abroad. Nor can there be any question that the electronic surveillance of foreign individuals located abroad who are reasonably believed to hold themselves out as agents and [redacted] of terrorist organizations targeting the United States is reasonable within the meaning of the Fourth Amendment. Efforts to monitor the activities of such individuals to detect and forestall possible terrorist attacks on this country present a paradigm case of a compelling government interest. The protections extended by the Fourth Amendment to foreign individuals abroad, if any, are minimal and plainly outweighed by the paramount national interest in preventing foreign attacks on our nation and its people.

But while the warrantless surveillance of foreign individuals abroad under the circumstances that existed here presents no cognizable constitutional problem, we must nevertheless still consider what protections the Fourth Amendment provides individuals located within the United States who communicate with the foreign individuals abroad lawfully targeted under Section 702.

The second Fourth Amendment principle implicated by incidental collection speaks directly to that concern. The Fourth Amendment generally is not violated when law enforcement officers, having lawfully undertaken electronic surveillance, whether under the authority of a warrant or an exception to the warrant requirement, discover and seize either evidence of criminal activity that they would not have had probable cause to search for in the first place, or the relevant conversations of an individual they did not anticipate or name in a warrant application. *See, e.g., United States v. Donovan*, 429 U.S. 413, 427 & n.15 (1977) (noting, as to domestic wiretaps, "[i]t is not a constitutional requirement that all those likely to be overheard engaging in incriminating conversations be named."); *United States v. Figueroa*, 757 F.2d 466, 472 (2d Cir. 1985) ("More particularly, the mere fact that Title III allows interception of

conversations of 'others as yet unknown' does not render the statute unconstitutional on its face as authorizing a general warrant.").

This line of cases has come to be known as the "incidental overhear" doctrine. *See, e.g., Suppression Decision*, 2016 WL 1029500 at *9 (noting that "[c]ourts have long dealt with the issue of incidental interception of non-targeted persons' communications" and collecting cases). Courts have repeatedly held that law enforcement agents do not need to obtain a separate warrant to collect conversations of persons as to whom probable cause did not previously exist with individuals whose oral or wire communications are being collected through a lawful wiretap or bug, where those conversations on their face contain evidence of criminal activity.[17] *See, e.g., Donovan*, 429 U.S. at 427 & n.15; *Figueroa*, 757 F.2d at 472; *see also In re Certified Question of Law*, 858 F.3d 605 (FISA Ct. Rev. 2016) (finding incidental collection of content information reasonable where warrant was obtained only for non-content dialing information); *United States v.*

[17] The "incidental overhear" doctrine is closely related to the "plain view" doctrine applied in connection with physical searches. *See, e.g., Coolidge v. New Hampshire*, 403 U.S. 443, 465-67 (1971) (describing plain view doctrine and noting that "[t]he doctrine serves to supplement the prior justification — whether it be a warrant . . . , hot pursuit, search incident to lawful arrest, or some other legitimate reason for being present unconnected with a search directed against the accused — and permits the warrantless seizure.").

Stewart, 590 F.3d 93, 129 (2d Cir. 2009) (concluding, in challenge to Title I FISA surveillance, that "[b]ecause Stewart's co-conspirators were targeted pursuant to proper procedures, the Fourth Amendment did not require that Stewart also be identified or described as a target in order for her intercepted conversations to be used in a criminal prosecution.") (internal citation omitted).

Combining these two Fourth Amendment principles, the government may lawfully collect, without a warrant and pursuant to Section 702, the e-mails of foreign individuals located abroad who reasonably appear to constitute a potential threat to the United States and, once it is lawfully collecting those e-mails, it does not need to seek a warrant, supported by probable cause, to continue to collect e-mails between that person and other individuals once it is learned that some of those individuals are United States citizens or lawful permanent residents, or are located in the United States. *Accord Mohamud*, 843 F.3d at 441; *see also United States v. Mohammad*, 339 F. Supp. 3d 724, 748-49 (N.D. Ohio 2018) (applying *Verdugo-Urquidez* and rejecting Fourth Amendment challenge to Section 702 surveillance where, despite marriage to United States citizen, defendant lived abroad at time of offense); *United States v. Muhtorov*, 187 F. Supp. 3d 1240, 1258 (D. Colo. 2015) (rejecting facial and as applied challenge to

incidental collection under Section 702 and concluding that a warrant was not acquired and search as reasonable). That is the case even if the government would have needed, but did not have, a warrant or probable cause had it sought to collect the e-mails of the American third party in the first instance. *Cf. In re Certified Question*, 858 F.3d at 604 (framing constitutional issue as whether incidental content collection rendered primary dialing information collection unreasonable, not whether warrant would have been required for content collection in its own right).

Objecting to this conclusion, Hasbajrami and *amici* advance several arguments seeking to apply the warrant requirement to Hasbajrami's case. Each is unavailing.

First, they argue that *Verdugo-Urquidez* does not control the outcome here because Section 702 collection occurs in the United States. Practically speaking, Section 702 surveillance could occur *only* within the United States, as the agencies can compel only ISPs located in the United States to provide e-mails.

But Fourth Amendment doctrine relating to wire or electronic communication does not focus on the location where the communication takes place. *Katz v. United States*, 389 U.S. 347 (1967), the seminal Supreme Court

decision on the interception of such communication, holds that a person's privacy interest in his or her communications does not depend on whether the government physically intrudes into a physical space in which that person has a property interest or an expectation of physical privacy. What matters, and what implicates the protection of the Fourth Amendment, is the expectation of privacy in the communications themselves, and therefore a warrant is required to seize even those communications made in a public telephone booth. Conversely, by the same reasoning, a person who does not have a Fourth Amendment-protected privacy interest in his communications, such as a foreign national resident abroad, does not acquire such an interest by reason of the physical location of the intercepting device. At least where the communication is collected essentially in real time as it occurs, the targeted communication, whether conducted over telephone wires or via the internet, occurs in the relevant sense where the person whose calls or e-mails are being intercepted is located, regardless of the location of the means used to intercept it.

Second, Hasbajrami argues that the surveillance cannot be properly considered "incidental" where the government can or even does expect to collect conversations with people with ties to the United States or located within its

borders. While we have concerns, expressed below, about the potential scope of Section 702 surveillance, those concerns are less applicable where, as here, collection and review are occurring nearly contemporaneously and that collection is ancillary to lawful surveillance of a permitted target. In the nature of law enforcement, there is always a possibility that the collection of evidence against a person who there is already probable cause to believe is involved in criminal activity or who is otherwise legitimately subject to surveillance will also develop information about others not previously reasonably suspected of wrongdoing. There is no contention here that the Section 702 surveillance was undertaken as a pretext to collect the communications of Hasbajrami, or of any other identified United States person or person located in the United States. That the overall practice of surveilling foreigners abroad of interest to the legitimate purpose of gathering foreign intelligence information may predictably lead to the interception of communications with United States persons no more invalidates that practice, or requires the government to cease its surveillance of the target until a warrant is obtained, than the general foreseeability of intercepting communications with previously unknown co-conspirators undermines the inadvertent overhear doctrine in ordinary domestic criminal wiretapping.

Finally, Hasbajrami and *amici* seek to distinguish the "incidental overhear" line of cases, noting that in those cases there was already an initial warrant supported by probable cause. They agree, however, that "the incidental overhear cases simply stand for the proposition that the government need not obtain *multiple* warrants to intercept protected communications." Brief of Amici Curiae American Civil Liberties Union and Electronic Frontier Foundation at 15, *United States v. Hasbajrami*, No. 15-2684 (2d Cir. Oct. 23, 2017) (emphasis in original). That is exactly the point here: once that initial surveillance is rendered lawful by a warrant, a FISC order, or some other exception to the warrant requirement, an additional warrant is not necessary in order to collect the calls or e-mails of third parties. As the district court recognized, once the surveillance was "lawful in the first place —whether it is the domestic surveillance of U.S. persons pursuant to a warrant or the warrantless surveillance of non-U.S. persons who are abroad — the incidental interception of non-targeted U.S. persons' communications with the targeted persons is also lawful." *Suppression Decision*, 2016 WL 1029500 at *9. The reason why the initial surveillance was lawful does not matter to this conclusion.

Accordingly, the incidental collection of United States persons' e-mails during lawful foreign intelligence surveillance of foreigners located abroad is not per se unreasonable because the collection is done without a warrant.

B. Incidental Collection of E-mails under Section 702 is Reasonable

Even absent a warrant requirement, however, the government's action must still be reasonable, at least insofar as it affects United States persons, to be consistent with the Fourth Amendment. *King*, 569 U.S. at 448. "To determine whether a search is reasonable under the Fourth Amendment, we examine the totality of the circumstances to balance, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate government interests." *In re Terrorist Bombings*, 552 F.3d at 172 (internal quotation marks omitted).

For the purposes of Hasbajrami's appeal, we may assume that a United States person ordinarily has a reasonable expectation in the privacy of his e-mails sufficient to trigger a Fourth Amendment reasonableness inquiry when the government undertakes to monitor even foreign communications in a way that can be expected to, and in fact does, lead to the interception of communications with United States persons. *See, e.g., United States v. Warshak*, 631 F.3d 266, 285-86

(6th Cir. 2010) (analogizing between letters and e-mails and finding reasonable expectation of privacy). In other words, we can assume that the government may not eavesdrop, without reasonable justification, on the conversations of United States persons (even abroad) with foreign nationals, simply because the United States person is interacting with a foreigner. Even assuming that a United States person might be understood to take some risk that the person with whom he or she is communicating is under surveillance, it does not follow that an American communicating with a foreign national must take the risk that the person with whom he is communicating is subject to unreasonable, or indiscriminate, electronic surveillance, or that communicating with foreigners subjects the American national himself or herself to continuing surveillance.

But such a privacy interest can be outweighed by the government's "manifest need to monitor" the communications of foreign agents of terrorist organizations operating abroad, and this need outweighs that interest in privacy and makes the incidental collection of communications between such foreigners and United States persons reasonable. *In re Terrorist Bombings*, 552 F.3d at 172. Even in the context of conventional warfare, identifying domestic agents of foreign powers is a principal concern of intelligence-gathering. The need to

identify potential domestic co-conspirators of hostile foreign persons or groups is even greater in the context of informal non-state terrorist organizations and movements. The recruitment of persons inside the United States or the placement of agents here to carry out terrorist attacks is one of the very threats that make it vital to surveil terrorist actors abroad. The communications of terrorist operatives abroad with persons inside the United States is thus of particular importance, and at least as important as monitoring the communications of foreign terrorists abroad among themselves.[18]

The logic of this conclusion is clear and compelling. If it is reasonable — and indeed necessary to the national security — for intelligence agencies to monitor the communications of suspected foreign terrorists abroad, the need to keep track of the potential threat from abroad does not lessen because some of the suspect's contacts turn out to be American nationals, or foreign nationals located within the United States. And when the conversations being monitored

[18] The same reasoning defeats any argument that such monitoring should be limited to the acquisition of foreign intelligence, and that communications collected for that purpose should not be made available to domestic law enforcement agencies. There is little point in having intelligence agencies collect information abroad if those agencies are not able to share what they learn with domestic law enforcement when the information they acquire points to ongoing or impending criminal activities inside our borders.

constitute evidence of criminal conspiracies between the foreign operative and someone located within the United States, the urgency becomes greater, not less. The logic of the plain view and inadvertent overhear cases fully applies: when an officer executing a lawful search or electronic surveillance warrant, or otherwise engaged in a lawful search, comes upon evidence of a previously unsuspected crime, or learns of the involvement of a previously unsuspected individual, the officer is not required to stop and obtain a new warrant to seize the item or to continue monitoring the phone line for which the warrant was obtained. The seizure of evidence of a crime in plain view without a warrant is a reasonable seizure. In the same way, when evidence of a potential crime involving an American comes to light during the lawful surveillance of a foreign operative abroad, it is entirely reasonable within the meaning of the Fourth Amendment for the government to continue monitoring the conversations of that operative with the American as well as with his or her other associates.[19]

[19] Of course, if the government wishes to expand the investigation to monitor the communications of the newly discovered United States-connected suspect, it would be required to obtain a conventional Title III or traditional FISA warrant [redacted]

In balancing Hasbajrami's privacy interest with the government's concern for national security, then, we conclude that the totality of the circumstances here weighs in the government's favor. The incidental collection of communications between targeted foreigners abroad and United States persons or persons in the United States is thus reasonable. For similar reasons, when the intelligence information properly collected raises reasonable grounds to believe that a crime is being committed or planned in the United States, dissemination of the information to a domestic law enforcement agency such as the FBI is also reasonable.

In summary, the district court reached the correct conclusions regarding incidental collection: the initial targeting of individuals without ties to the United States and located abroad is lawful; there is no need for a warrant in order to collect incidental communications by United States persons to and from those individuals; and both the collection of such communications and the dissemination of information from such collection about potential criminal actions within the country to domestic law enforcement are reasonable under the Fourth Amendment. Were such incidental collection the only Section 702 material relevant to Hasbajrami's motion, we would simply affirm the district

court's ruling. But, as the record currently stands, we must also consider additional issues.

II. "Inadvertent" Collection

The district court's ruling on the suppression motion did not address whether any e-mail accounts of United States persons or individuals within the United States, including Hasbajraini, had been "inadvertently" targeted, that is, targeted by mistake under the presumption that an address was controlled by a non-United States person.

Upon reviewing the classified record, in particular its *ex parte* proceedings under the Classified Information Procedures Act ("CIPA"), 18 U.S.C. app. 3, § 1 *et seq.*, it is clear that the district court was made aware of one instance of the direct targeting of an e-mail account controlled by a United States person that resulted in the collection of Hasbajrami's communications. Before the incidental collection discussed above, the NSA had directly targeted at least one such e-mail address. Like the later incidental collection, the NSA had originally been monitoring communications with individuals it reasonably believed were non-United States persons located abroad, and as a result discovered an e-mail from the United States person. At that time, however, NSA analysts concluded, wrongly, that the

account holder was not a United States person. The NSA therefore tasked the account (a different account than those that were the subject of incidental collection detailed above) in its own right, and collected communications from the account for several weeks. The agency eventually detasked the account after it concluded it was not yielding significant intelligence information, but it did not initially purge the information because it did not discover until later that the account holder was a United States person. The related Section 702-acquired material, which included communications to and/or from Hasbajrami, stayed in NSA databases, however, and was not disseminated to domestic law enforcement, until the agency conducted a search of these databases in 2014 following the initiation of Hasbajrami's prosecution.

The inadvertent collection of communications raises complicated questions. First, as a statutory matter, Section 702 prohibits the targeting of e-mail accounts that the government knows to be maintained by United States persons. *See* 50 U.S.C. § 1881a(b). But the statute thus appears to prohibit only knowing or intentional targeting, and not to address situations where the government is mistaken, reasonably or unreasonably. Does the express prohibition of targeting accounts known to be those of United States persons

implicitly authorize the targeting of any account not known with certainty to be that of a United States person? If there is evidence of a high likelihood that the account belongs to a United States person and the government proceeds to target it without taking steps to investigate further, does the willful blindness standard, which equates such deliberate indifference to actual knowledge in many legal contexts, apply? *Cf. Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 766-69 (2011) (discussing willful blindness doctrine).

Second, the Fourth Amendment calculus for such collection would be different than the one employed in considering incidental collection. Incidental collection is justified because the "target" of the surveillance cannot rely on the Fourth Amendment's protections, as discussed above. But a United States citizen or lawful permanent resident, located in the United States, assuming a reasonable expectation of privacy, would be protected by the Fourth Amendment. Is the Fourth Amendment prohibition of "unreasonable" searches violated if the government unreasonably (recklessly or negligently) concludes that the targeted account is that of a foreigner located abroad? Is it permissible for the government to adopt a presumption that, under all circumstances or in the presence of one or more key indicia, an account holder whose identity is

unclear should be treated as foreign? Would the later discovery that the account did indeed belong to a United States person require the minimization, or the suppression in a criminal case, of inadvertently collected conversations?

A district court reviewing a motion to suppress evidence inadvertently collected (or derived from inadvertent collection) would have to address these issues, and perhaps others, in deciding whether the government's reliance on inadvertent collection in an investigation or prosecution was reasonable within the meaning of the Fourth Amendment.

But we need not decide those questions today because we are satisfied that any inadvertent collection disclosed to the district court was harmless. The interception of communications from the inadvertently targeted account was brief, lasting only approximately two weeks. The materials collected, whatever they were, were not used in applying for the FISA warrant — indeed, their very existence seems to have been unknown to anyone involved in the criminal investigation of Hasbajrami, as the inadvertent targeting of the account in question was not even discovered by the government until well into the prosecution of this case. And finally, the collection was terminated because the government itself determined that nothing of any intelligence value was being

learned. Presumably that conclusion would not have been reached if the collected conversations were indicative of criminal terrorist plots, or were of evidentiary value to a criminal investigation.

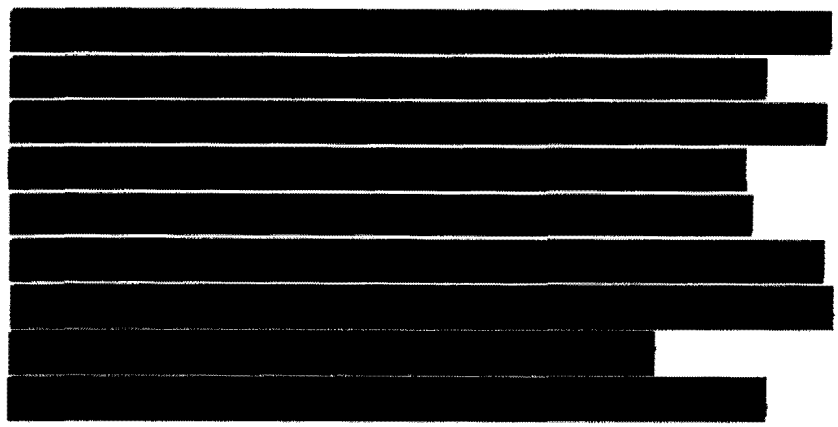
Thus, even assuming *arguendo* that there was some legal infirmity in the decision to begin collection despite uncertainty about the status of the account, or to continue it once at least some evidence pointing to a possible United States source for the account was discovered, we conclude, even in the context of a conditional guilty plea, that the failure to suppress the results of that collection was harmless beyond any reasonable doubt.

III. Querying

There is a third issue in this case, however: the storage of Section 702 information in databases and the subsequent querying of those databases by the government. The district court did not make any findings regarding whether the NSA, the FBI or any other agency queried databases with regard to Hasbajrami prior to the FISC order. Instead, it appeared to accept the government's argument, framed within the context of a discussion of whether the minimization procedures provided adequate protections so as to make *collection* reasonable, that the government could freely query information it had lawfully acquired

without further Fourth Amendment inquiry. *See Suppression Decision*, 2016 WL 1029500 at *12 n.20 ("I agree with the government that it would be perverse to authorize the unrestricted review of lawfully collected information but then restrict the targeted review of the same information in response to tailored inquires.") (internal alterations and quotation marks omitted).

The government renewed this argument on appeal. Following oral argument, during which the government would neither confirm nor deny whether it had queried any databases of Section 702-acquired information, this Court ordered further briefing. The government [redacted]



Gov't Supplemental Classified Br. at 6-7 (emphasis added). [redacted]

Like inadvertent collection, the storage and querying of information raises challenging constitutional questions, to which there are few clear answers in the case law. *Cf. In re Directives*, 551 F.3d at 1015 (dismissing petitioner's concerns, under the PAA, because the "government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons, and there is no evidence to the contrary."). The issue was not addressed by the Ninth Circuit in *Mohamud*, which explicitly left open the question of whether "the incidental overhear doctrine permits the unconstitutional and widespread retention and querying of the incidentally collected information," stating that the issue was "not before [the court]." 843 F.3d at 440 n.24. The district court in *Mohamud* did reach the question, however, and it concluded that the "subsequent querying of a § 702 collection, even if U.S. person identifiers are used, is not a separate search and does not make § 702 surveillance unreasonable under the Fourth Amendment." *United States v. Mohamud*, No. 3:10-cr-475-KI-1, 2014 WL 2866749, at *26 (D. Or. June 24, 2014), *aff'd*, 843 F.3d 420 (9th Cir. 2016).

We do not find that logic persuasive. Storage has little significance in its own right: the lawfully-collected communications, even of United States persons, continue to serve the same foreign intelligence purpose in the continued

surveillance of a foreign operative, whether his interlocutor is a United States person or a citizen and resident of some other country. The material is justifiably retained, not to keep tabs on a United States person, but to keep tabs on the non-United States person abroad who has been targeted.[20]

But querying that stored data does have important Fourth Amendment implications, and those implications counsel in favor of considering querying a separate Fourth Amendment event that, in itself, must be reasonable. Our reasoning is based on three considerations.

First, courts have increasingly recognized the need for additional probable cause or reasonableness assessments to support a search of information or objects that the government has lawfully collected. It is true that the FBI does not need an additional warrant to go down to its evidence locker and look through a box of evidence it collected from a crime scene. But lawful collection alone is not always enough to justify a future search.

In *Riley v. California*, the Supreme Court held that a warrant was necessary to search a cell phone, even when that cell phone was lawfully seized pursuant to

[20] The considerations might be different if the storage involved data responsive to a warrant and retained for the purpose of a domestic criminal prosecution. This Court, sitting *en banc*, considered similar issues in *United States v. Ganias*, 824 F.3d 199 (2d Cir. 2016), although we ultimately did not need to decide them.

a search incident to a lawful arrest. 573 U.S. 373, 401 (2014). Several circuit court decisions have reached similar conclusions. In *United States v. Sedaghaty*, for instance, the government had searched a defendant's home pursuant to a warrant focused on tax violations. 728 F.3d 885, 912 (9th Cir. 2013). Agents seized nine computers, which forensic experts searched with "an evolving list of search terms" in order "to comb through the computers for useful materials," eventually finding evidence confirming the defendant was supporting Chechen terrorist groups. *Id.* The Ninth Circuit concluded that the searches beyond the scope of the warrant were improper, noting that the government "should not be able to comb through [the defendant's] computers plucking out new forms of evidence that the investigating agents have decided may be useful" after it failed to find evidence of willfulness regarding the tax returns. *Id.* at 913. To do so required a new warrant, even though the government already had access to the machines and had lawfully seized them. *See also United States v. Runyan*, 275 F.3d 449, 464-65 (5th Cir. 2001) (finding that police exceeded the scope of a private search when they "examined disks that the private searchers did not examine" and would have required a warrant to do so); *United States v. Mulder*, 808 F.2d 1346, 1349 (2d Cir. 1987) (holding that a separate warrant was needed to test

packages in suitcase for drugs, even though the suitcase was lawfully seized via private search).

Second, Section 702 is sweeping in its technological capacity and broad in its scope. In the case of the incidental collection discussed above, [redacted] was collecting and reviewing e-mails for its own foreign intelligence purposes in [redacted], and reporting [redacted] evidence that it obtained suggesting on-going criminal activity in the United States. Such activity is closely analogous to precedents drawn from traditional domestic criminal wiretapping. As discussed above, it is not difficult to conclude that, like "incidentally overheard" criminal conversations and evidence of crimes seized in plain view, the collection and use of information obtained in this way is reasonable within the meaning of the Fourth Amendment.

But the vast technological capabilities of the Section 702 program, estimated by the PCLOB as totaling nearly 250 million e-mails annually by 2011 and likely larger numbers since then, may mean that analysts are not reviewing each of those e-mails contemporaneously with their collection. PCLOB Report at 116, 128-29. If such a vast body of information is simply stored in a database, available for review by request from domestic law enforcement agencies solely

on the speculative possibility that evidence of interest to agents investigating a particular individual might be found there, the program begins to look more like a dragnet, and a query more like a general warrant, and less like an individual officer going to the evidence locker to check a previously-acquired piece of evidence against some newfound insight.

The Supreme Court has expressed increasing concern about the interaction between Fourth Amendment precedent and evolving government technological capabilities. *Riley* rested in part on the fact that "[c]ell phones . . . place vast quantities of personal information literally in the hands of individuals." 573 U.S. at 386. "A search of the information on a cell phone [therefore] bears little resemblance to the type of physical search considered" in past cases. *Id.*; *see also Ganias*, 824 F.3d at 217-18 (noting privacy implications of expansive technology and data storage). And in *Carpenter*, the Court concluded that a warrant (or a valid substitute) was required to acquire cell-site records, even though they were stored by a third party and under traditional Fourth Amendment doctrine a cellphone user would not have an expectation of privacy in such information:

> We decline to grant the state unrestricted access to a wireless carrier's database of physical location information. In light of the deeply revealing nature of [this information], its depth, breadth, and

> comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection. The Government's acquisition of the cell-site records here was a search under that Amendment.

Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

Third, as a practical matter, querying is problematic because it may make it easier to target wide-ranging information about a given United States person at a point when the government knows it is investigating such a person. Section 702 forbids the government from targeting a non-United States person as a backdoor way of targeting a United States person. 50 U.S.C. § 1881a(b). But, as detailed above, in the course of its intelligence gathering operations, the NSA may have collected all sorts of information about an individual, the sum of which may resemble what the NSA would have gathered if it had directly targeted that individual in the first place. To permit that information to be accessed indiscriminately, for domestic law enforcement purposes, without any reason to believe that the individual is involved in any criminal activity and or even that any information about the person is likely to be in the database, just to see if there is anything incriminating in any conversations that might happen to be there, would be at odds with the bedrock Fourth Amendment concept that law

enforcement agents may not invade the privacy of individuals without some objective reason to believe that evidence of crime will be found by a search. Treating querying as a Fourth Amendment event and requiring the query itself to be reasonable provides a backstop to protect the privacy interests of United States persons and ensure that they are not being improperly targeted.

Fourth, much may depend on who is querying what database. There is a potentially significant difference between, for example, the FBI querying its own database and the FBI requesting that the NSA query its far larger archive of collected communications, collected pursuant to a broader mandate. As we understand the public sources of information about the collection and use of Section 702 material, the FBI maintains its own records of communications provided to it by the NSA. *See* PCLOB Report at 58-59. Such communications presumably were provided because review of the material properly collected by the NSA under Section 702 uncovered evidence of criminal activity (relating to terrorism or otherwise), and were appropriately communicated to domestic law enforcement. Just as the FBI may act on such information where it requires immediate criminal investigation, it may well be appropriate for the agency to retain the information and store it for later review when other legitimate

evidence or leads make that information relevant to an on-going investigation. Such a review of the agency's own files is arguably analogous to traditional law enforcement techniques; evidence lawfully collected does not always accumulate to a sufficient quantity to warrant an immediate arrest or indictment, but may be retained and later reviewed when additional evidence is developed. FBI queries directed to a larger archive of millions of communications collected and stored by the NSA for foreign intelligence purposes, on the chance that something in those files might contain incriminating information about a person of interest to domestic law enforcement, raise different concerns.

What kinds of querying, subject to what limitations, under what procedures, are reasonable within the meaning of the Fourth Amendment, and when (if ever) such querying of one or more databases, maintained by an agency of the United States for information about a United States person, might require a warrant, are difficult and sensitive questions. We do not purport to answer them here, or even to canvass all of the considerations that may prove relevant or the various types of querying that may raise distinct problems.

Indeed, we cannot do so on the sparse record presented. We do not know what databases were queried by whom, for what reasons, what (if any)

information was uncovered by such queries, or what (if any) use was made of any information uncovered. The government has represented that no information derived from any such queries was presented to the FISC to obtain the FISA warrant, but has not addressed whether any such information contributed to the investigation in other ways. [redacted]

Given these considerations, the district court here must conduct an inquiry into whether any querying of databases of Section 702-acquired information using terms related to Hasbajrami was lawful under the Fourth Amendment. For today we need only reiterate that "the ultimate touchstone of the Fourth Amendment is reasonableness." *Riley*, 573 U.S. at 381; *cf. Abu-Jihaad*, 630 F.3d at 121-22 (stating that, even in the application of the warrant requirement, the requirement is "flexible, so that different standards may be compatible with the Fourth Amendment in light of the different purposes and practical considerations at issue.") (internal quotation marks and citations omitted).

We cannot, and should not, go further, pending development of a more complete record by the district court on remand, and an assessment by the

district court as to whether whatever was done was consistent with the Fourth Amendment and whether, if there was any illegality, any evidence should have been suppressed in response to Hasbajrami's motion.[21]

IV. Hasbajrami's Conditional Plea and Resolution of the Motion to Suppress

As addressed above, there is still an open issue as to what queries of Section 702-acquired information occurred in this case, whether any such queries were reasonable and, if unreasonable, whether the queried information tainted the application before the FISC or in some other way would lead to the suppression of any evidence.

But in its post-argument briefing, the government argues that even if it did query Section 702 databases, that action ultimately could not matter because the

---

[21] On November 14, 2019, Hasbajrami filed a Rule 28(j) letter alerting this Court to three recently declassified opinions from the FISC and FISCR. *See In re DNI/AG 702(h) Certifications 2018*, 941 F.3d 547 (FISA Ct. Rev. 2019); *Redacted* (FISA Ct. Sep. 4, 2019); *Redacted*, 2018 WL 9909971 (FISA Ct. Oct. 18, 2018). Based on our review, we do not believe that these opinions substantively affect our decision because, even to the extent that their approach differs from ours, they are not binding on this Court. Since we are remanding for the district court to further assess this issue with the benefit of a more complete record, we decline to engage further at this time. We did not find it necessary to review the unredacted versions of these opinions in reaching this conclusion and, therefore, Hasbajrami's request for access to the unredacted versions of these opinions is DENIED.

communications collected as a result of incidental collection would provide an independent source sufficient to support the FISC's probable cause determination. Gov't Supplemental Classified Br. at 9 (arguing that "this Court's analysis should be limited to alleged 'searches' where a causal link can be drawn between the search and the acquisition of the evidence that Hasbajrami seeks to suppress.").

The government relies primarily on *Murray v. United States*, 487 U.S. 533 (1988). In *Murray*, federal law enforcement agents surveilling the defendant witnessed him drive into a warehouse in South Boston. *Id.* at 535. Agents arrested the defendant and a co-conspirator after they drove away from the warehouse and, upon arrest, the agents discovered marijuana in the defendant's truck. The agents then forced entry into the warehouse, where they "observed in plain view numerous burlap-wrapped bales that were later found to contain marijuana. They left without disturbing the bales, kept the warehouse under surveillance," and re-entered only after obtaining a warrant. *Id.* In applying for the warrant, however, the agents did not advise the court of their prior entry; they also did not rely on their observations of the contents of the warehouse in order to establish probable cause. *Id.* at 536. The Supreme Court held that

suppression of the evidence eventually seized from the warehouse would not be required "if the warrant-authorized search of the warehouse was an independent source of the challenged evidence." *Id.* at 543-44. Although "[k]nowledge that the marijuana was in the warehouse was assuredly acquired at the time of the unlawful entry . . . it was also acquired at the time of entry pursuant to the warrant, and if that later acquisition was not the result of the earlier entry there is no reason why the independent source doctrine should not apply." *Id.* at 541.

Even assuming the government was querying databases simultaneously with its incidental collection activities, according to the government's position its agents would be analogous to the agents in *Murray*. Their subjective understanding of the evidence might have been affected by the fruits of an unreasonable search, and had they relied on that evidence in support of a warrant application they might not be able to use the evidence obtained by executing that warrant. But, according to the government, if the information they placed before the FISC, and that court's subsequent probable cause determination, rested on other information, that "later acquisition was not the result of the earlier [search]" and so "there is no reason why the independent source doctrine should not apply." *Id.* at 541.

We cannot apply the independent source doctrine on the record currently before us. Had this case gone to trial, our task would be significantly different. Under those circumstances, we could have undertaken to trace, as the Ninth Circuit did in *Mohamud*, 843 F.3d at 438 & n.21, individual pieces of evidence that had *actually* been presented to the jury at that trial in order to assess whether those pieces of evidence had been obtained consistent with the Fourth Amendment. And if individual pieces of evidence needed to be suppressed, the Court could then decide whether the admission of any given piece of evidence was harmless when compared to all the legally obtained evidence that was ultimately presented at trial.

But we are not reviewing the acquisition of evidence used at a trial. Rather, Hasbajrami's appeal reaches us following a conditional plea made pursuant to Rule 11(a)(2) of the Federal Rules of Criminal Procedure. Rule 11(a)(2) provides that:

> With the consent of the court and the government, a defendant may enter a conditional plea of guilty or nolo contendere, reserving in writing the right to have an appellate court review an adverse determination of a specified pretrial motion. A defendant who prevails on appeal may then withdraw the plea.

According to the Advisory Committee Notes to the 1983 Amendments, conditional pleas should be permitted "only when the decision of the court of appeals will dispose of the case either by allowing the plea to stand or by such action as compelling dismissal of the indictment or suppressing essential evidence." *See also United States v. Bundy*, 392 F.3d 641, 647-48 (4th Cir. 2004). The classic example of a case in which that standard is met is a narcotics case in which the evidence sought to be suppressed is the very basis of the charge. The suppression of the evidence would end the case; if the evidence is admissible, guilt is assured; if not, no evidence of guilt remains. The situation is more problematic and complicated, however, where the suppression of some but not all of the evidence in the case is a possible outcome.

Our sister circuits have applied a harmless error calculation when evaluating whether an opportunity to withdraw a plea is a necessary remedy after it is determined on appeal that the challenged district court ruling was, in whole or in part, erroneous. *See, e.g., United States v. Lustig*, 830 F.3d 1075, 1086 (9th Cir. 2016); *United States v. Rivera-Nevarez*, 418 F.3d 1104 (10th Cir. 2005) (affirming conviction on harmless error where conviction was upheld on

grounds not considered by district court).[22] Those courts have applied the harmless error rule by asking "whether the erroneous suppression ruling could have affected [the defendant's] decision to plead guilty." *Lustig*, 830 F.3d at 1086.

But the record here is murky. It is clear that the presence or absence of Section 702 surveillance affected Hasbajrami's initial decision to plead guilty. Indeed, it was because the district court was convinced that Hasbajrami's initial decision to plead guilty was predicated in part on his lawyers' assurance that the government had represented that there was no warrantless surveillance in his case that it granted the defense motion to withdraw Hasbajrami's first guilty plea when those representations were revealed to have been inaccurate. App'x at 39 (noting that Hasbajrami "specifically asked [his counsel] about whether warrantless wiretaps had played a role in his case. After they informed him that such wiretaps were not part of the evidence, he was more willing to plead guilty."). Moreover, Hasbajrami moved to suppress *all* Section 702 material

---

[22] The Advisory Committee also considered Fed. R. Crim. P. 11(h)'s harmless error calculus to apply, but it noted that, without full factual development, invocation of the harmless error rule would be difficult. The Committee noted, however, that "relatively few appellate decisions result in affirmance upon [harmless error]. Thus it will only rarely be true that the conditional plea device will cause an appellate court to consider constitutional questions which could otherwise have been avoided by invocation of the doctrine of harmless error." Fed. R. Crim. P. 11, advisory committee's notes to 1983 amendments.

collected by the government, including matter that was not presented to the FISC to obtain the traditional FISA warrant. What is unclear is just how much Section 702-acquired information would remain, after further fact-finding at the district court. It may be that, after a full evaluation of the record in light of Hasbajrami's motion to suppress, the evidence available to the government remains very much intact. For all we know, any queries conducted by the government may have been entirely reasonable, they may not have yielded any evidence at all, and any material that was uncovered even by a putatively unconstitutional query may not have affected the investigation in any way.

However those matters would be decided on remand, though, we cannot predict here whether any such queries were constitutionally questionable, or whether any information derived from such queries should itself have been suppressed, or directly or indirectly tainted the warrant application. And, without being able to fully predict or decide either of those issues, we also cannot adequately predict whether a potentially-altered evidentiary landscape "could have affected [Hasbajrami's] decision to plead guilty." *Lustig*, 830 F.3d at 1086; *see also United States v. Leake*, 95 F.3d 409, 420-421 (6th Cir. 1996) (noting that Fed. R. Crim. P. 11(a)(2) addresses the situation in which "the defendant is fully

successful on appeal," and not "the effect of a *partially* successful appeal," but vacating judgment because "[defendant was] successful in excluding what appears to be the most damning evidence against him.") (emphasis in original).

Taking these considerations into account, then, we are left with a posture similar to that faced by this Court in *United States v. Wong Ching Hing*, 867 F.2d 754 (2d Cir. 1989). The defendant in that case had reserved his right to appeal the district court's failure to suppress roadside statements made to police without Miranda warnings, as well as subsequent statements made at a police station. *Id.* at 756. This Court, like the district court, found that the roadside statements were voluntary and that suppression was therefore unnecessary as to those. *Id.* But the defendant had made two separate sets of statements to law enforcement once detained at the police station. The first set was made to the state police, and it did not add anything to what he had voluntarily provided at the initial stop. The second set of statements, however, was made to a DEA agent and "formed the basis of the information to which Wong pled guilty," which charged him with making a false statement. *Id.*

The Court concluded that the circumstances "may well warrant the conclusion that the detention was not valid as a *Terry* stop." *Id.* at 758. But it was

unclear what effect such a holding would have on Wong's legal position, because the record was not clear as to whether the conditional guilty plea was "conditioned upon the government's being successful in *admitting all of the statements or any one of them*." *Id.* at 758 (emphasis added). The Court therefore vacated the judgment and remanded to the district court for "further proceedings," noting that the government had also urged affirmance on an alternative ground and that "the parties will not be precluded from asserting new arguments" on remand. *Id.*

We therefore follow a similar course of action here. Because the district court was not even aware whether such querying had occurred, and because even we have not been advised as to what was done, for what reasons, and with what results, we remand to the district court to determine the facts, consistent with the considerations stated above, and to decide in the first instance, based on its factual findings, whether there was a constitutional violation in this particular case, and what (if any) evidence would need to be suppressed if there was indeed a violation. Similarly, we leave it to the district court to determine, in the first instance, whether any exceptions to the exclusionary rule, such as a good

faith exception, might apply in this case.[23] Finally, we leave it to the district court to determine, if any evidence should have been suppressed, whether the failure to suppress that evidence was harmless, and if it was not what remedy is appropriate.

On remand, the district court should undertake whatever proceedings are necessary, consistent with the considerations stated above. To the extent that any decisions must be made about what information is to be presented to appropriately-cleared defense counsel, such decisions too are best left to the district court after it becomes clear what the inquiry about querying will involve.[24] *Cf. Abu-Jihaad*, 630 F.3d at 129 (noting that, under FISA, disclosure is

---

[23] The government has argued before this Court that the good faith exception would apply. Because of the incomplete record here, we take no position as to whether the exception applies.

[24] Hasbajrami argues on appeal that his due process rights would be violated if he is not provided with an unredacted or unmodified version of the district court's order. He concedes, however, that the argument would be rendered moot if this Court reverses on either constitutional or statutory grounds. After reviewing the minor redactions, we conclude that the limited information redacted from the district court's opinion could not have substantially affected Hasbajrami's due process rights in this appeal. In any event, we undertook *de novo* review and we are satisfied that the limited redactions in the portions of this opinion relating to the district court's rulings do not require disclosure to the defense at this time. We therefore deny Hasbajrami's request to unseal or to disclose to the defense team the redacted portions of the district court opinion. As addressed above, however, the district court remains free to consider, in the

exception and *ex parte*, in camera review is the rule, and that the review of materials that are "relatively straightforward and not complex" may not necessarily require adversarial testing).

CONCLUSION

Based on the foregoing considerations, we REMAND to the district court for further proceedings consistent with this opinion.

---

first instance, what if any classified material, including the government's Rule 28(j) letter and the redacted portions of this opinion relating to querying, should be provided to properly-cleared defense counsel on remand, consistent with the requirements of CIPA and FISA. We therefore DENY Hasbajrami's February 8, 2019 motion for disclosure of the government's Rule 28(j) letter, without prejudice to renewal before the district court on remand.